Biztonság és védelem az informatikában

5. gyakorlati feladat

Készítette: Baranyi Gábor
CRC7FC

2021.03.18.

Windows, Linux Hardening

Hardening: általában a rendszer biztonságossá tétele a sérülékenységi felület csökkentésével, amely nagyobb, ha a rendszer több funkciót lát el, elvileg az egyfunkciós rendszer biztonságosabb, mint a többcélú.

Választott két website-om:

https://www.newnettechnologies.com/how-to-harden-your-cloud-environment-in-5-steps.html

https://securityboulevard.com/2020/07/web-system-hardening-in-5-easy-steps/

A két site között az a legnagyobb különbség, hogy a securityboulevard.com részletesebben lépésekre szedettebben mutatja be a hardening-et, mint a newnettechnologies.com.

securityboulevard.com

Lépésenként részletes leírásokkal mutatja be, hogy web system hardening-et megteremtsük.

1. Az operációs rendszer hardening

   Az oldal szerint első lépés az operációs rendszer biztonságossá tétele.

2. Hálózat hardening

   A kiszolgáló szintjén sokat lehet tenni a hardening érdekében.

3. Web szerver hardening

   A szerver elsődleges feladata a webalkalmazások tárolása a web szerverek hardening-jére is kell összpontosítani

4. Web alkalmazás hardening

   Legnagyobb probléma a webalkalmazásokhibái melyek az internetes biztonsági résekből következnek ezek kiküszöbölése a legfontosabb.

5. Folyamatos hardening

   Nem elég kialakítani folyamatosan fel is kell tartani.

newnettechnologies.com

Az oldal ismerteti a hardening fogalmát majd tanácsokat ad az elkezdéséhez. Ezeket követően 5 lépésben leírja mit kell csinálni.

Legkevesebb hozzáférés

- **Least Access** - Restrict server access from both the network and on the instance, install only the required OS components and applications, and leverage host-based protection software.

Legkevesebb kiváltság

- **Least Privilege** - Define the minimum set of privileges each server needs in order to perform its function.

Konfiguráció-menedzsment

- **Configuration Management** – Create a baseline server configuration and track each server as a configuration item. Assess each server against the current recorded baseline to identify and flag and deviations. Ensure each server is configured to generate and securely store appropriate log and audit data.

Változáskezelés

- **Change Management** – Create processes to control changes to server configuration baselines.

Napló

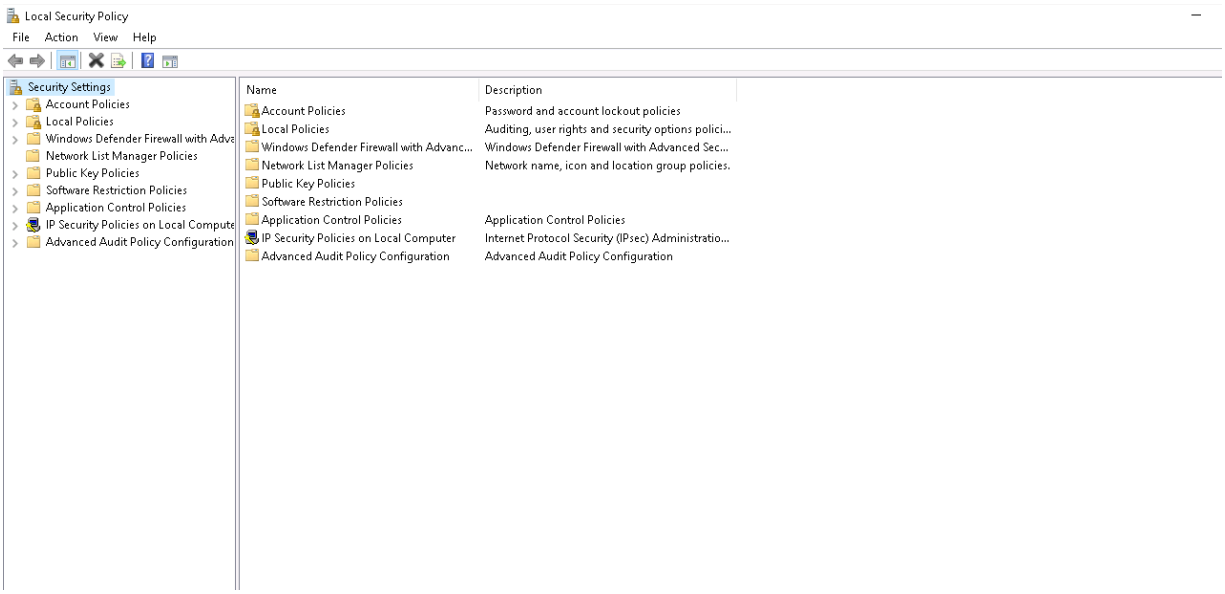
- **Audit Logs** – Audit access and all changes to EC2 instances to verify server integrity and ensure that only authorized changes are made.

Az oldal még a felhő tárhelyünk hardening-jére is hasznos tanácsokat ad, míg a másik oldal csak 1 témára koncentrált.

Windows server 2019 hardening esetén elvégzendő beállítások:

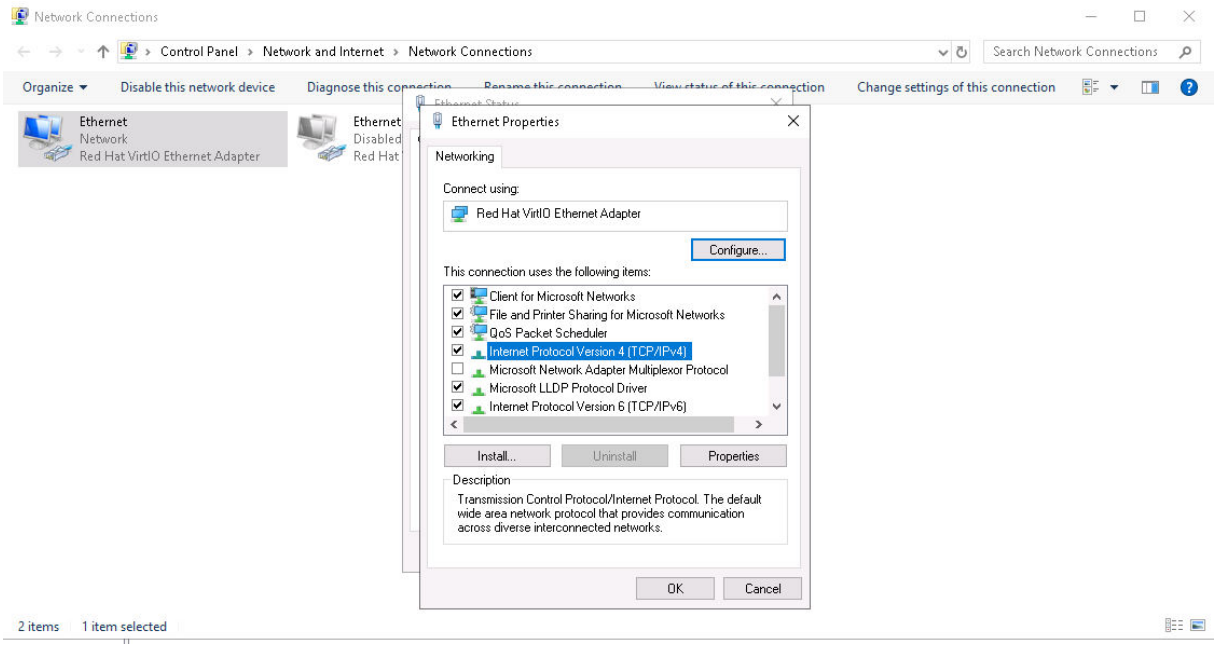
User Configuration:

Fontos, hogy a helyi rendszergazdai fiók jelszava biztonságos legyen. Ehhez hasonlóan minden lehetséges esetben le kell tiltani a helyi rendszergazdát.



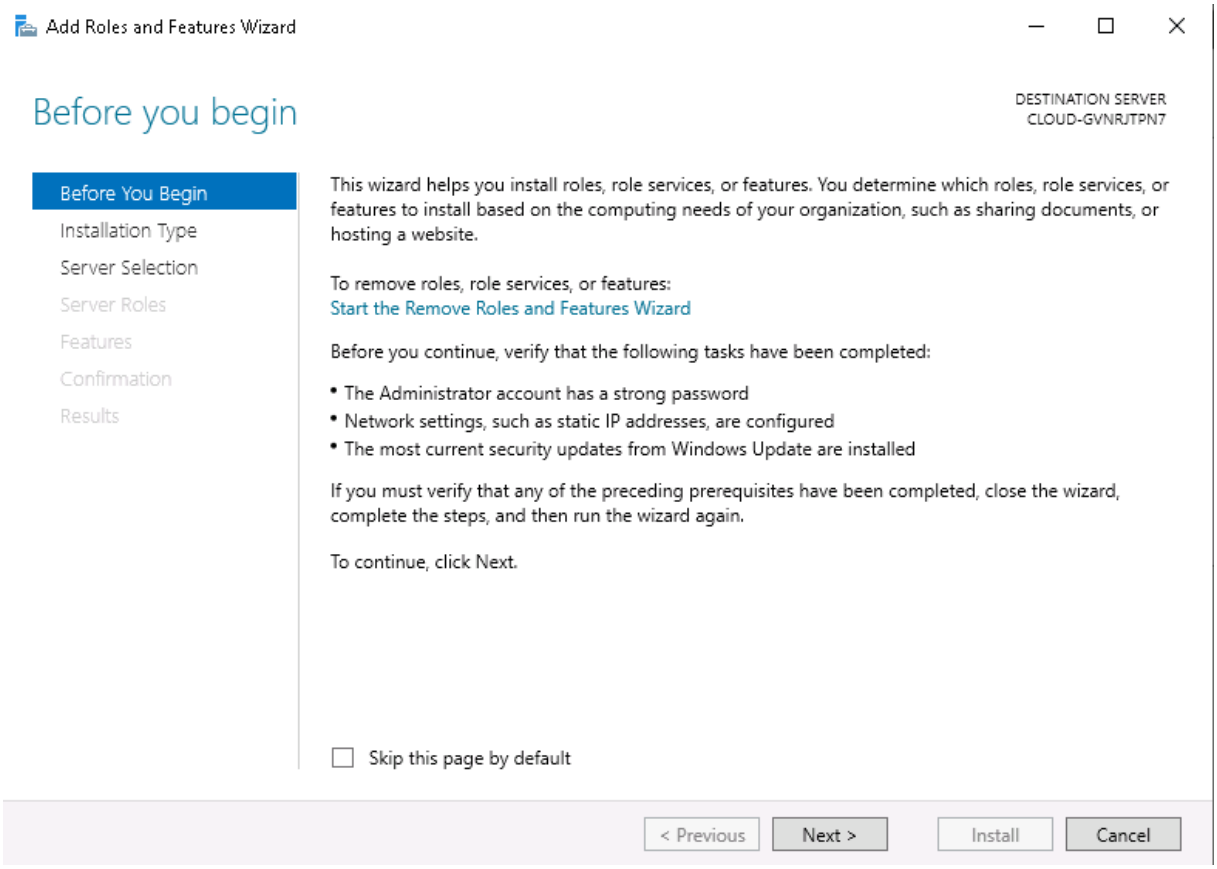
Network Configuration

A termelési kiszolgálóknak statikus IP-t kell használniuk. Ilyen esetben az ügyfelek megbízhatóan megtalálják őket. Az IP-nek védett szegmens formátumúnak kell lennie, amelyet tűzfal véd.



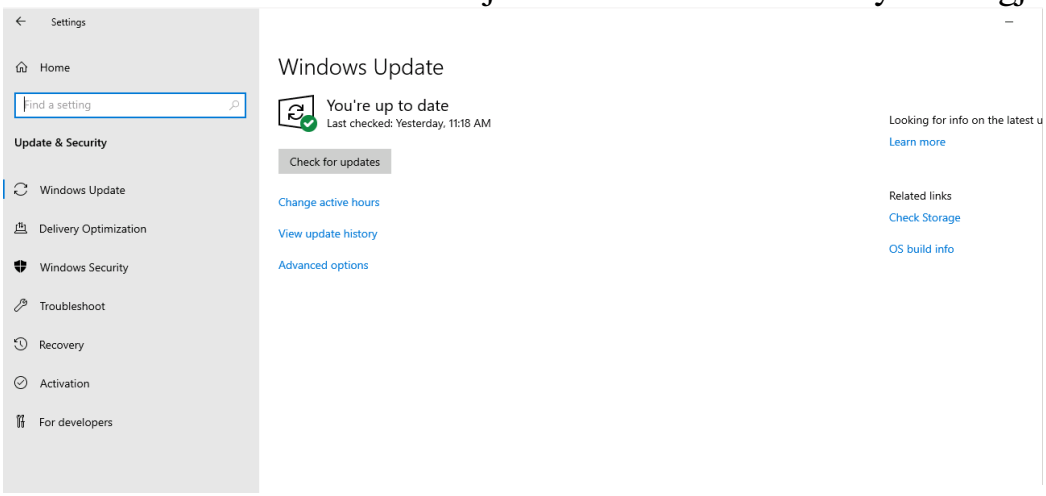
Windows Features and Roles Configuration

A szolgáltatások és szerepkörök használatához a Microsoft operációs rendszer csomagokat használ. A szerepek meghatározhatók olyan tulajdonságok gyűjteményeként, amelyeket egy meghatározott célra hoztak létre. A szerepeket akkor választják meg, ha egy szerver be tudja őket fogadni. A funkciók ettől a ponttól testre szabhatók.



Update Installation

A kiszolgáló biztonságának legfinomabb módja a naprakészség. Ez nem túl nehéz. Nem kell frissítéseket és javításokat alkalmazni milyent megjelennek.

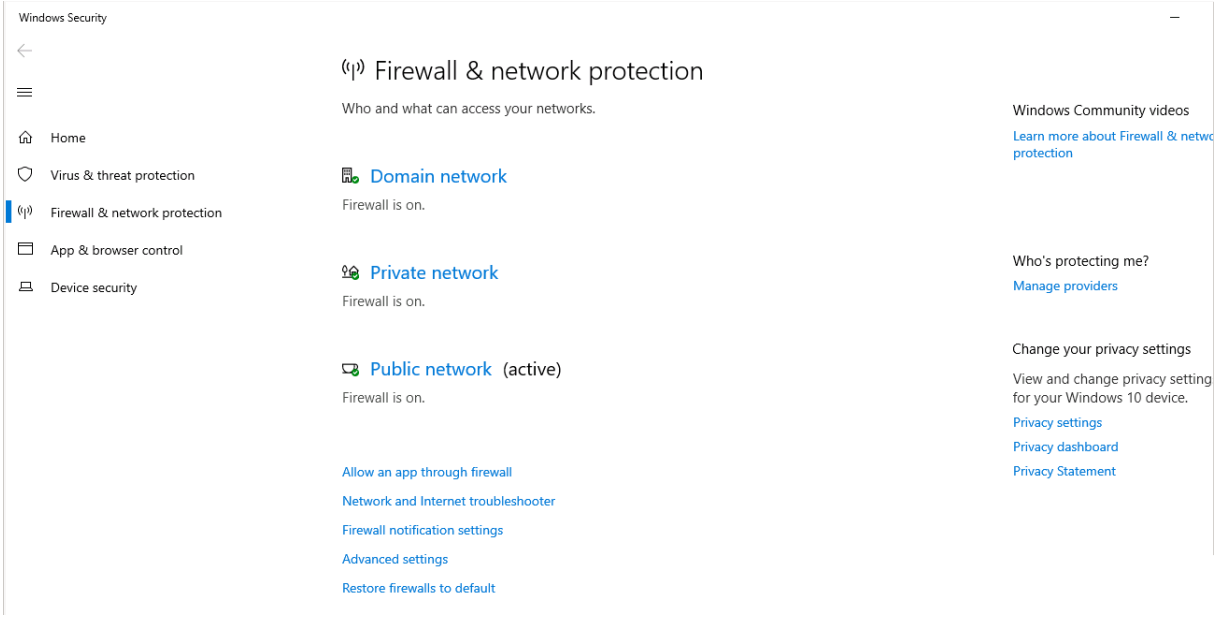


NTP Configuration

Még akkor is, ha csupán öt perces időeltolódás lép fel, a Windows bejelentkezéseit teljesen lebontják. Ugyanez vonatkozik számos más olyan funkcióra, amelyek a Kerberos biztonságára támaszkodnak.

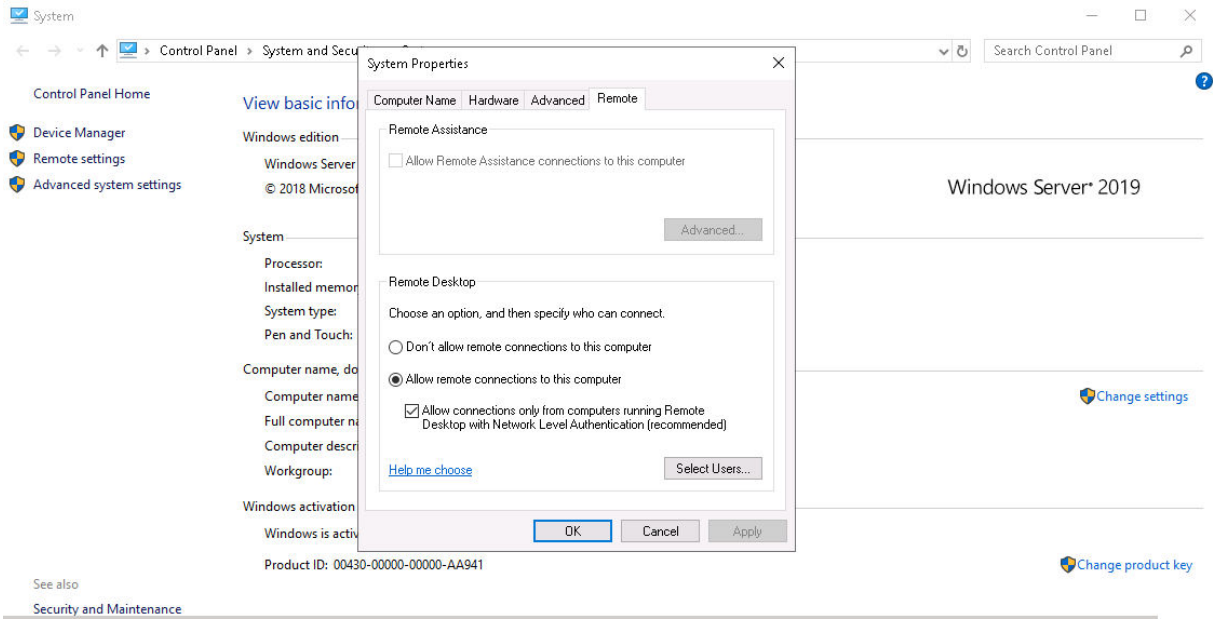
Firewall Configuration

A webkiszolgáló felépítéséhez csak webportokra van szükség. A 80-as és 443-as portoknak nyitva kell lenniük, és létre kell hozniuk a kapcsolatot a szerver és az internet között.



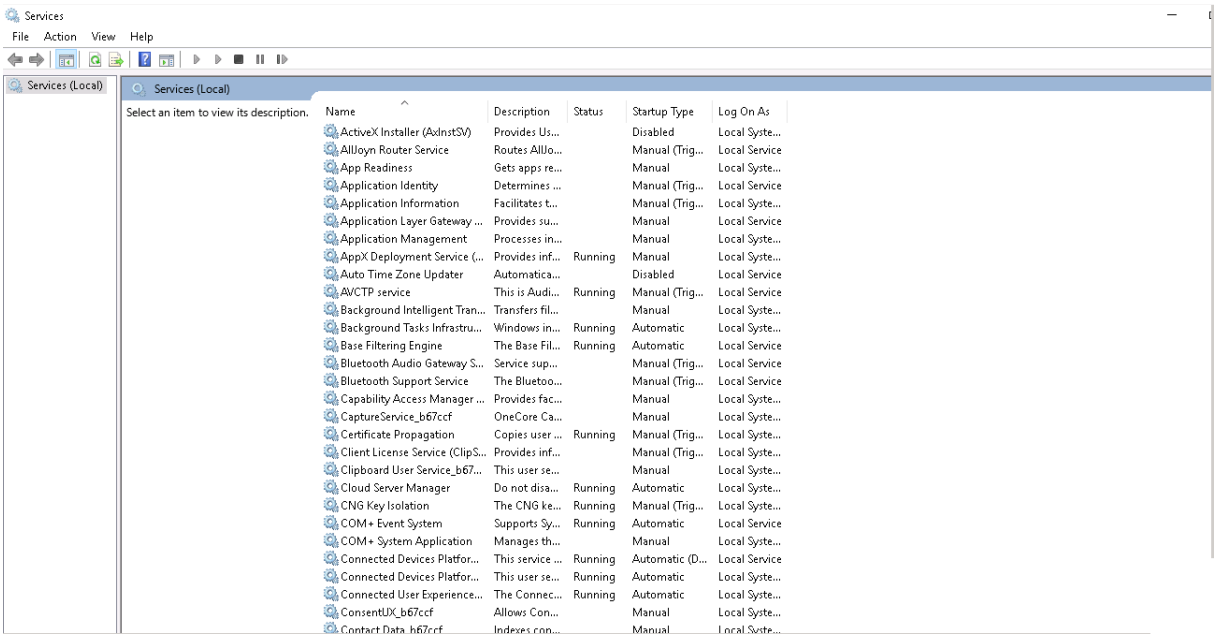
Remote Access Configuration

Ha valaki RDP-t használ, annak csak VPN-en keresztül kell elérhetőnek lennie. Ez is csak abban az esetben van, ha az akadálymentesítés egyáltalán lehetséges.



Service Configuration

A Windows szerveren alapértelmezett szolgáltatások állnak rendelkezésre. Automatikus indításkor a háttérben futnak.



Windows 10 client hardening esetén elvégzendő beállítások:

Alap elvek:

Az illetéktelen fizikai hozzáférés elleni védelem érdekében a merevlemezt titkosítani kell.

Az integrált Windows Defender megoldás vírusirtó szoftverként használható. A Windows Defender megfelelő védelmet nyújt az ismert rosszindulatú programok ellen, és nem találtak súlyos gyengeségeket.

2009-ben a Microsoft kiadta az Enhanced Mitigation Experience Toolkit (EMET) alkalmazást, amely a mélység védekezésében használható a sebezhetőségek kiaknázása ellen. Az EMET intézkedéseket tartalmaz olyan ismert kiaknázások ellen, mint a kupacszórás és a Return Oriented Programming.

A Windows 10 rendszerben a Windows Update tulajdonságai megváltoztak. Bizonyos idő elteltével a Windows frissítései automatikusan települnek, és a rendszer újraindul.

Védelem és Biztonság:

Az NT LAN Manager (NTLM) használata szintén a biztonsággal kapcsolatos téma a Windows 10 számára. Ha a támadó képes rögzíteni az NTLM kihívás válaszfolyamatát, például a hálózati forgalom manipulálásával, akkor ezt felhasználhatja a felhasználó jelszavának kidolgozására. A nyolcjegyű jelszó néhány óra alatt kidolgozható. Az NTLM mostantól csak a 2. verzióban használható (NTLMv2); az összes többi verziót (NTLMv1 és LM) el kell utasítani. Ideális esetben az NTLM-et teljesen deaktiválni kell, vagy csak meghatározott IP-címekre kell korlátozni

Egy új biztonsági funkció blokkolja a megbízhatatlan betűtípusokat (truetype betűtípusok), de az alapértelmezett beállításokban nem aktív.

A Windows 10 számos olyan funkcióval rendelkezik, amelyek az alapértelmezett beállításokban negatívan befolyásolják a felhasználó magánéletét.

ELLENŐRZÉS ÉS NAPLÓK:

A biztonsággal kapcsolatos eseményeket rögzített rendszeren kell naplózni és értékelni. Ehhez ki kell bővíteni az alapértelmezett beállításokat.

A támadási kísérlet vagy a hozzáférési adatokkal való visszaélés korai felismerése érdekében a sikertelen bejelentkezési kísérleteket naplózni kell. A naplóbeállítások megerősítése azonban csak akkor segít, ha a naplók integritása biztosított, és azokat megfelelően rögzítették.

Ezért az eseménynapló maximális méretét ki kell bővíteni annak biztosítása érdekében, hogy felülírással egyetlen bejegyzés sem veszhet el.

Ezenkívül a hozzáférési jogokat az adminisztrátorokra kell korlátozni.

Linux hardening eseén elvégzendő beállítások:

1. Telepítsen biztonsági frissítéseket és javításokat

A rendszerek legtöbb gyengeségét a szoftver hibái okozzák. Ezeket a hibákat biztonsági réseknek nevezzük. A szoftveres javítások kezelésének megfelelő gondozása segít csökkenteni a kapcsolódó kockázatokat.

2. Használjon erős jelszavakat

A rendszer fő átjárója az, hogy érvényes felhasználóként jelentkezik be a fiók kapcsolódó jelszavával.

3. Kösse a folyamatokat a localhosthoz

Nem minden szolgáltatásnak kell rendelkezésre állnia a hálózaton keresztül. Például amikor a MySQL helyi példányát futtatja a webkiszolgálón, hagyja, hogy csak egy helyi socketen hallgasson, vagy kapcsolódjon a localhosthoz.. Ezután konfigurálja az alkalmazást úgy, hogy ezen a helyi címen keresztül csatlakozzon, amely általában már az alapértelmezett.

4. Tűzfal telepítése

Csak az engedélyezett forgalomnak szabad ideális helyzetben elérnie a rendszerét. Ennek megvalósításához valósítson meg egy olyan tűzfalmegoldást, mint az iptables vagy az újabb nftable.

5. Tartsa tisztán a dolgokat

Minden olyan rendszerre telepített program, amely nem tartozik oda, csak negatívan befolyásolhatja a gépét.

Megvalósítható feladatok a következők:

Törölje a fel nem használt csomagot

Tisztítsa meg a régi otthoni könyvtárakat, és távolítsa el a felhasználókat

6. Biztonságos konfigurációk

A legtöbb alkalmazás egy vagy több biztonsági intézkedéssel rendelkezik, amelyek megvédik a szoftvert vagy a rendszert fenyegető bizonyos formákat.

7. Korlátozza a hozzáférést

Csak engedélyezett felhasználók számára engedélyezheti a géphez való hozzáférést.

8. Figyelje a rendszereit

A legtöbb behatolást nem észlelik, az ellenőrzés hiánya miatt. A normál rendszerfigyelés és a biztonsági események felügyeletének végrehajtása. Például a Linux audit keretrendszer használata növelte a feltételezett események észlelési arányát.

9. Készítsen biztonsági másolatokat (és teszteljen!)

Rendszeresen készítsen biztonsági másolatot a rendszeradatokról. Ez megakadályozhatja az adatvesztést. Még ennél is fontosabb: tesztelje a biztonsági másolatokat. A biztonsági másolat készítése szép, de a visszaállítás számít!

10. Végezze el a rendszer auditálását

A leírtak alapján kikövetkeztethető, hogy mind a linux, mind a windows hardening egyaránt védelmet nyújt az illetéktelen programok és behatolók ellen, de továbbra sem nyújtanak 100%-os védelmet.

Források:

https://www.webservertalk.com/windows-server-2019-hardening-checklist-guide/

https://linux-audit.com/linux-server-hardening-most-important-steps-to-secure-systems/

https://www.scip.ch/en/?labs.20161215

https://securityboulevard.com/2020/07/web-system-hardening-in-5-easy-steps/

https://www.newnettechnologies.com/how-to-harden-your-cloud-environment-in-5-steps.html

https://en.wikipedia.org/wiki/Hardening_(computing)